

Response

Applicant: Kevin R. Driscoll

Serial No.: 09/712,505

Filed: November 14, 2000

Docket No.: H16-26353 (H162.104.101)

Title: CRYPTOGRAPHIC COMBINER USING TWO SEQUENTIAL NON-ASSOCIATIVE OPERATIONS

REMARKS

This is responsive to the Office Action mailed July 1, 2004. Claims 1-43 were rejected. Claims 1-43 remain pending in the application and are presented for reconsideration and allowance.

Claim Rejections under 35 U.S.C. § 102

The Examiner has rejected claims 1-43 for being anticipated by the Ritter U.S. Patent No. 4,979,832 under 35 U.S.C. § 102(b).

Independent claims 1, 9, 18, and 31 all include limitations related to providing a keystream and cryptographically combining a first binary data sequence and the keystream and performing two sequential non-associative operations on the first binary data sequence and the keystream to provide the second binary data sequence. Independent claim 1 includes both an encryption combiner and a decryption combiner in a stream cipher cryptosystem. Independent claim 9 includes a cryptographic combiner (which could be an encryption combiner as claimed in dependent claim 10 or a decryption combiner as claimed in dependent claim 11) in a stream cipher cryptosystem. Independent claim 18 claims a method of encrypting a plaintext binary data sequence. Independent claim 31 claims a method of decrypting a ciphertext binary data sequence.

The Ritter patent does not teach or suggestion cryptographically combining a first binary data sequence and the keystream and performing two sequential non-associative operations on the first binary data sequence and the keystream to provide a second binary data sequence as included in the limitations of independent claims 1, 9, 18, and 31.

By contrast, the Ritter patent discloses a dynamic substitution combiner and extractor. In the Ritter patent, a plaintext value on input 10 is transformed by substitution 12 into a ciphertext value output 14. A ciphertext value on input 22 is transformed by substitution 24 into the original plaintext value on output 26. Substitution 12 must be invertible to make this work. For example, the substitution table in substitution 12 can be made exactly as large as the number of possible input values 10 and filled sequentially with the possible output values. If no output

Response

Applicant: Kevin R. Driscoll

Serial No.: 09/712,505

Filed: November 14, 2000

Docket No.: H16-26353 (H162.104.101)

Title: CRYPTOGRAPHIC COMBINER USING TWO SEQUENTIAL NON-ASSOCIATIVE OPERATIONS

value appears more than once, substitution 12 will be invertible. Substitution 12 can then be shuffled or randomized in any number of ways, as long as the values in the table in substitution 12 are re-arranged or permuted, substitution 12 will remain invertible. Typically, substitution 12 is implemented as addressable storage and realized with an electronic memory device, or an addressable area of memory hardware in an electronic digital computer or microprocessor. The substitution changes controller 18 uses both substitution input 10 and combiner substitution changes input 16 to change the content of substitution 12 by way of combiner substitution changes controls 20.

Thus, the Ritter patent dynamic substitution combiner and extractor device is similar to the very complex cryptographic combiner discussed in the Background of Invention section of the present application. As stated in the Background of Invention section of the present application, one example cryptographic combiner in this very complex category is a permutation table combiner, wherein the permutation table is required to have a table the size of the plaintext alphabet. As stated in the present application at page 12, lines 14-17, since each combiner operation according to the present invention is substantially the same complexity as the XOR and other linear combiner operations, there is not the extensive expense in time, hardware and/or software resources of conventional very complex combiner operations (such as the dynamic substitution combiner extractor disclosed in the Ritter patent).

Moreover, the Ritter patent actually teaches away from the present invention, as the Ritter patent, at column 3, lines 7-9 states that the "alternative of selecting some other simple Boolean logic function to replace the exclusive-OR combiner does not work."

In view of the above, the Ritter patent does not teach or suggest the stream cipher cryptosystems of independent claims 1 and 9, the method of encrypting of independent claim 18, or the method of decrypting of independent claim 31. In addition, dependent claims 2-8 further define patentably distinct independent claim 1, dependent claims 10-17 further define patentably distinct independent claim 9, dependent claims 19-30 further define patentably distinct independent 18, and dependent claims 32-43 further define patentably distinct independent claim 31. Therefore, these dependent claims are also believed to be allowable.

Response

Applicant: Kevin R. Driscoll

Serial No.: 09/712,505

Filed: November 14, 2000

Docket No.: H16-26353 (H162.104.101)

Title: CRYPTOGRAPHIC COMBINER USING TWO SEQUENTIAL NON-ASSOCIATIVE OPERATIONS

Therefore, Applicant respectfully requests that the rejections to claims 1-43 under 35 U.S.C. § 102 be withdrawn and that these claims be allowed.

CONCLUSION

In view of the above, Applicant respectfully submits that pending claims 1-43 are in form for allowance and are not taught or suggested by the cited references. Therefore, reconsideration and withdrawal of the rejections and allowance of claims 1-43 is respectfully requested.

The Examiner is invited to contact the Applicant's representative at the below-listed telephone number to facilitate prosecution of this application.

No fees are required under 37 C.F.R. 1.16(b)(c). However, if such fees are required, the Patent Office is hereby authorized to charge Deposit Account No. 500471.

Response

Applicant: Kevin R. Driscoll

Serial No.: 09/712,505

Filed: November 14, 2000

Docket No.: H16-26353 (H162.104.101)

Title: CRYPTOGRAPHIC COMBINER USING TWO SEQUENTIAL NON-ASSOCIATIVE OPERATIONS

Any inquiry regarding this Amendment and Response should be directed to either Patrick G. Billig at the below-listed telephone numbers or Kris T. Fredrick at Telephone No. (763) 954-5388. In addition, all correspondence should continue to be directed to the following address:

HONEYWELL INTERNATIONAL, INC.

Law Department AB2

P.O. Box 2245

Morristown, New Jersey 07962-9806

Respectfully submitted,

Kevin R. Driscoll,

By his attorneys,

DICKE, BILLIG & CZAJA, PLLC

Fifth Street Towers, Suite 2250

100 South Fifth Street

Minneapolis, MN 55402

Telephone: (612) 573-2003

Facsimile: (612) 573-2005

Date: 10-1-04

PGB:cmj




Patrick G. Billig

Reg. No. 38,080

CERTIFICATE UNDER 37 C.F.R. 1.8:

The undersigned hereby certifies that this paper or papers, as described herein, are being deposited in the United States Postal Service, as first class mail, in an envelope address to: Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on this 1 day of October, 2004.



By _____
Name: Patrick G. Billig